Future X Communications

FXC3009
Management Guide

2008 年 12 月

FXC株式会社

本マニュアルについて

■ 本マニュアルでは、FXC3009 の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI （コマンドラインインタフェース）または Web ブラウザで行います。

■ このマニュアルには、事故を防ぐための重要な注意事項と本製品を使う前の必要な準備について説明しています。まず、この取扱説明書をよくお読みのうえ、安全に製品をご使用ください。お読みになったあとは、いつでも見られるところに必ず保管してください。




この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、必ず最初にお読みください。

⬩下記事項は、安全のために必ずお守りください。



● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

⬩煙が出たら

⬩異常な音、においがしたら

⬩内部に水・異物が入ったら

⬩製品を高所から落としたり、破損したとき

①電源を切る（電源コードを抜く）
②接続ケーブルを抜く
③販売店に修理を依頼する

- 下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。



● 電源ケーブルや接続ケーブルを傷つけない

- 電源ケーブルを傷つけると火災や感電の原因となります。
- 重いものをのせたり、引っ張ったりしない。
- 加工したり、傷つけたりしない。
- 熱器具の近くに配線したり、加熱したりしない。
- 電源ケーブルを抜くときは、必ずプラグを持って抜く。

● 内部に水や異物を入れない

- 火災や感電の原因となります。
- 万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。

● 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。

● 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。

製品取り扱い時のご注意

- 下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。



● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。

● 指定の電圧で使う

マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

- 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
- 毛足の長いジュウタンなどの上に直接設置しない。
- 布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

目次

1. コマンドラインインタフェース

1.1 コマンドラインインタフェースへのアクセス

コンソールポートへの接続は以下の手順で行います。

(1) **本機のコンソールポートと、**PC **のシリアルポートを、コンソールケーブルで繋ぎます。**

(2) **ターミナルソフトウェアを起動します。設定を以下の通り行ってください。**

通信ポート ----------- RS-232C **ケーブルが接続されているポート**
(COM **ポート** 1 **又は** COM **ポート** 2)
通信速度 -------------- 38400 **ボー** (baud)
データビット -------- 8bit
ストップビット ----- 1bit
パリティ -------------- **なし**

(3) **本機の電源を入れます。**
接続が確立されると初期化が行われた後、以下の画面が表示されます。

```
Booting Program Version 1.02.00, built at 08:42:45, Mar 30 2004

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05900000, 16 blocks of 0x00010000 bytes
each.
==> enter ^C to abort booting within 3 seconds ......


Start to run system initialization task.
[System Configuration]
Company Name      :
Model Name        : 10-port Intelligent Switch
MAC  Address      : 00:C0:F6:63:01:5E




Firmware version: 2.20.14 (built at Sep 19 2005 10:34:25)
Press <ENTER> key to start.
UCD-SNMP version 4.1.2

Username:
Password:
```

(4) "Enter" **キーを押すと、ユーザー名とパスワードが要求されます。**
ユーザー名、パスワードの変更を行っていない場合には以下の値を入力してくださ

Username:admin / Password:123456

[注意] 安全のために CLI へログイン後 P7 「admin ー管理ユーザ設定」コマンドを使用してパスワードの変更を行ってください。

(5) **スイッチにログイン後、プロンプトが表示されます。**
"?" **または** "help" **コマンドで、本機で使用可能なコマンドリストを確認することができます。**

例

```
10-port Intelligent Switch>help
[Command List]
?.............. Help commands
backup......... backup run-time firmware or configuration file
del............ Del commands
find........... Find commands
exit........... Logout
help........... Help commands
logout......... Logout
ping........... Ping a specified host with IP address
reset.......... Reset system or reset factory default setting
set............ Set commands
show........... Show commands
upgrade........ Upgrade run-time firmware or configuration file
```

※ Telnet **接続経由での管理も、コンソール接続と同じインタフェースを使用します。**

1.2 コマンド

1.2.1 基本コマンド

backup ーバックアップ

本機は TFTP プロトコルによる、ファームウェア及び設定ファイルのダウンロード・アップロードをサポートしています。

まずファームウェアまたはコンフィグレーションを選択し、TFTP サーバの IP アドレス、バックアップを行うファイル名を指定します。

文法

backup [firmware | config] { *IP address* } { *filename* }

- firmware | config - ファームウェア、設定ファイルのどちらかを指定します。
- *IP address* - TFTP サーバーの IP アドレスを指定します。
- *filename* - ファイル名の指定。任意の文字列を入力します。

例

```
10-port Intelligent Switch>backup firmware 192.168.1.10 config_backup
Start to upload run-time firmware file......OK.
```

logout (exit) ーログアウトコマンド

ログイン中のユーザーからログアウトし、セッションを終了します。

logout と exit は同様の動作を行います。

例

```
10-port Intelligent Switch>logout




Press <ENTER> key to start.

Username:
```

Ping コマンド

ネットワーク上の他のノードにたいし、ICMP echo **リクエストを送信します。**

文法

ping -n {*count* } **-l** { *length*} **-t -w** { *timeout* } *ip address*

- **-n** {*count* } - **送信するパケット数を指定**
- **-l** { *length*} - **パケットのサイズを指定**（64~8148bytes）
- **-t** - **この引数を付けると、「**Esc**」キーを押すまで** Ping **を送信し続けます。**
- **-w** { *timeout* } - **各応答までの待ち時間を指定（ミリ秒）**
- *ip address* - **送信先** IP **アドレス**

例

ノード「192.168.1.7**」へ** 175bytes **のパケットを** 1 **回送信します。**

```
10-port Intelligent Switch>ping -n 1 -l 175 192.168.1.7
PING server 192.168.1.7
175 bytes from 192.168.1.7: icmp_seq=0, time<10ms
Sent 1 packets, received 1 OK, 0 bad
```

Reset

本機の再起動及び、設定を工場出荷状態に戻す際に使用します。

文法

reset [configuration **|** system]

- configuration - **設定内容を工場出荷状態に戻し、再起動を行います。**
- system - **本機の再起動を行います。設定内容は保持されます。**

例

本機の再起動を行います。

```
10-port Intelligent Switch>reset system
Reset system ......
10-port Intelligent Switch>+
Booting Program Version 1.02.00, built at 08:42:45, Mar 30 2004

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05900000, 16 blocks of 0x00010000 bytes each.
==> enter ^C to abort booting within 3 seconds ......

Start to run system initialization task.
[System Configuration]
Company Name      :
Model Name        : 10-port Intelligent Switch
MAC  Address      : 00:C0:F6:63:01:5E
```

1.2.2 各種コマンド

admin －管理ユーザ設定

管理者のユーザー名とパスワードを変更します。

文法

set admin

初期設定

username ：admin

password ：123456

例

ユーザー名を「fxc123」パスワードを「56789」に変更します。

```
10-port Intelligent Switch>set admin

Input Old Username: admin
Input Old Password:

Input New Username: fxc123
Input New Password:
Confirm Password:
Successful to set new username and password!
```

[注意] 安全の為、初期設定パスワードの変更を行ってください。

[注意] 入力したパスワードは表示されません。

arl ー ARL テーブル

本機の持つ ARL テーブルへ、MAC アドレスを静的に追加します。

本コマンドで作成した ARL テーブルを基に、“set security” コマンドの設定が反映されます。

"del arl" コマンドにより、登録した MAC アドレスを削除できます。

“show arl“ コマンドを使用して、現在の ARL テーブルの内容を確認できます。

文法

set arl {*MAC Adress* } {*port#*} [high **|** Low]

del arl {*MAC Adress* }

find arl {*MAC Adress* }

show arl [all **|** static **|** dynamic]

- *MAC Adress* - MAC **アドレスを指定**
- *port#* - **ポート番号を指定**
- high **|** Low - **プライオリティ（高 / 低）**
- **find arl** - ARL **テーブルから、**MAC **アドレスを検索します。**
- **show arl** - ARL **テーブルを表示します。**all= **全て、**static= **静的** ARL **テーブル、**dynamic= **動的** ARL **テーブル**

例

ARL テーブルにポート 6 の静的 MAC ID”00-00-01-02-03-35” を ”Low” プライオリティで追加します。

```
10-port Intelligent Switch>set arl 00-00-01-02-03-35 6 low
Successful!
```

ポート 5 の静的 MAC ID”00-00-01-02-03-33” を削除します。

```
10-port Intelligent Switch>del arl 00-00-01-02-03-33
Successful!
```

静的 ARL テーブルを表示します。

```
10-port Intelligent Switch>show arl static

 --- Static Address List ---
  ID   Priority  Mac Address        PORT
   1     Low     00-00-01-02-03-35   6
   2     Low     00-C0-F6-11-22-33   7
```

ARL テーブルから MAC アドレス ”00-C0-F6-11-22-33” を検索します。

```
10-port Intelligent Switch>find arl 00-c0-f6-11-22-33
This MAC [00-c0-f6-11-22-33] is in port [ 7 ]!
```

関連する項目

security ーセキュリティ（P26）

eth0 ー IP 設定

IP **アドレスに関連した設定を行います。**

設定内容を確認する場合には “show net“ **コマンドを使用します。**

文法

set eth0 ip {*IP address*} **netmask** {*netmask* } **gateway** {*gateway*}

show net

- **ip** {*IP address*} - IP **アドレスを指定**
- **netmask** {*netmask* } - **サブネットマスクを指定**
- **gateway** {*gateway*} - **デフォルトゲートウェイのアドレスを指定**
- **show net** -IP **アドレス関連の設定内容を表示。**

[注意] 本機に接続するノードが、同じサブネット上にない場合は、デフォルトゲートウェイの設定が必要です。

初期設定

IP Address：192.168.1.5

Netmask ：255.255.255.0

Gateway ：192.168.1.120

例

IP **アドレスを** 192.168.2.35**、サブネットマスクを** 255.255.255.0**、デフォルトゲートウェイを** 192.168.2.254 **に設定しています。**

```
10-port Intelligent Switch>set eth0 ip 192.168.2.36 255.255.255.
10-port Intelligent Switch>
10-port Intelligent Switch>set eth0 ip 192.168.2.35 netmask
255.255.255.0 gatewa
y 192.168.2.254
Set IP address successful!
Set default gateway successful!
10-port Intelligent Switch>show net
[eth0] Network Configuration:
IP Address: 192.168.2.35
Netmask   : 255.255.255.0
Gateway   : 192.168.2.254
```

idle ーアイドルタイム

本機では、CLI または Web インターフェースでの操作が一定時間行われなかった場合、自動的にログアウトを行う機能を備えています。本コマンドで、自動ログアウトが行われるまでの時間を設定できます。

文法

set idle { *timeout value* }

- *timeout value* - 自動ログアウトを実行するまでの秒数を指定します（30-3600 秒）

初期設定

600 秒（10 分）

例

自動ログアウトの時間を 20 分（1200 秒）に設定します。

```
10-port Intelligent Switch>set idle 1200
Set idle time 1200 seconds successfully.
```

igmp ー IGMP 機能

IGMP 機能を設定します。設定内容を確認する場合には "show igmp" コマンドを使用します。

文法

set igmp [enable | disable] **routerport** {*Port#*}

set igmp routerport {*Port#*}

show igmp

- enable | disable - IGMP snooping 機能を有効 / 無効にします。
- **show igmp** - IGMP snooping 設定情報を表示します。
- **routerport** {*Port#*} - ルーターポート番号を指定します。

初期設定

disable（無効）

例

IGMP snooping を有効にし、ルータポートを 8 に設定します。その後に IGMP 情報を表示します。

```
10-port Intelligent Switch>set igmp enable
IGMP function is enabled!
10-port Intelligent Switch>set igmp routerport 8
IGMP Router Port is 8.
10-port Intelligent Switch>show igmp
[IGMP Configuration]
IGMP Switch      : Enabled
IGMP Router Port: 8
Total Groups     : 0
```

mirror ーポートミラーリング

ポートミラーリングはネットワーク管理者にトラフィックの監視機能を提供します。監視対象のポートからパケットのコピーが転送され、監視をおこなうポートがこれらすべてのパケットを受信し、指定したポートでトラフィックの監視が可能になります。

文法

set mirror ingress div {*value*} **mode** [all | sa | da] **mac** {*MAC Address*} **monitor** {*Port#*}

set mirror egress div {*value*} **mode** [all | sa | da] **mac** {*MAC Address*} **monitor** {*Port#*}

- **ingress - 入力パケットのキャプチャ**
- **egress - 出力パケットのキャプチャ**
- **div** {*value*} **- 全トラフィックのうち、採取するパケットの割合を指定。**"10" **と指定した場合、**10 **パケット毎に** 1 **つのパケットのみを採取。全てのパケットを採取する場合には** "1" **を指定。**
- **mode** [all | sa | da] **- モニタリングするパケットのモードを選択します。**

  all **：全てのパケットをモニタリング。**
  sa **：送信元** MAC **アドレスを指定してモニタリング。**
  da **：宛先** MAC **アドレスを指定してモニタリング。**

- **mac** {*MAC Address*} **- モニタリングする送信元** / **送信先の** MAC **アドレスを指定（**mode **で** SA **または** DA **を選択した場合のみ）**
- **monitor** {*Port#* } **- 被モニタリングポート（監視ポート）を指定します。**"," **で区切ることにより、複数のポートを指定可能です。**

set mirror port {*Port#* }

- {*Port#* } **- モニタリングポート（監視ポート）を指定します。（**1 **ポート）**

set mirror [enable | disable]

- [enable | disable] **- ポートミラーリング機能の有効** / **無効を指定。**

del mirror

- **ポートミラーリング機能を無効にします。**

show mirror

- **ミラーポートの設定情報を表示します。**

初期設定

ミラーリング機能：disable**（無効）**

例

ポートミラーリング機能を有効にし、ポート 5,6,7 **番から出る全パケットの内、送信先** MAC **アドレスが** 00-c0-f6-11-22-33 **のパケットをポート** 8 **番にてモニタリングします。**
その後、ミラーポートの設定情報を表示しています。

```
10-port Intelligent Switch>set mirror enable
Enable mirror function successful!
10-port Intelligent Switch>set mirror port 8
Set mirror capture port successful!
Mirror capture port = 8
10-port Intelligent Switch>set mirror egress mode da mac 00-c0-
f6-11-22-33 monitor 5,6,7
Set Egress mode successful!
Set Egress mac successful!
Set Egress monitor port successful!
Egress Monitor Port List: 5 6 7
10-port Intelligent Switch>show mirror
[Mirror Configuration]
Mirror Switch:Enabled
Capture port :8
Ingress DIV=1     Mode=ALL  MAC=00-00-00-00-00-00
        Port List:
Egress  DIV=1     Mode=DA
        Port List: 5 6 7
```

age ーエージングタイム

MAC アドレスのエージングタイムを設定します。

文法

age { *time* }

- *time* - エージングタイムを指定（0-65535 秒　0：エージング機能の無効）

初期設定

300 秒

例

MAC アドレスエージングタイムを 600 秒（10 分）に設定します。

```
10-port Intelligent Switch>set age 600
Switch Age      : Enabled
Switch Age Time : 600 (seconds)
```

automode ーオートモード

ポートのオートモード機能を設定します。本機には 2 種類のオートモードがあります。

- an mode - auto negotiation mode
  対向の機器のオートネゴシエーション機能が無効になっている場合は an mode を選択します。
- ad mode - auto detection mode
  対向の機器のオートネゴシエーション機能が有効の場合は ad mode を選択します。どちらのモードを選択するかは、各ネットワーク構成によって異なります。ほとんどのケースでは ad モードが推奨されています。

文法

set automode [an | ad]

show automode

- an - オートネゴシエーションモード
- ad - オートディテクションモード

初期設定

Auto Detect

例

オートモードをオートディテクションモードに設定します。

```
10-port Intelligent Switch>set automode ad
Set auto mode as "Auto Detect" successful!
```

port ーポート設定

本コマンドは、各ポートの設定を行います。
“show port“ **コマンドにて、ポートの設定状況及び、接続状態を表示します。**

文法

set port { *port#* } **name** {*name*} **admin** [enable | disable] **speed** [atuo | 10 | 100 | 1000] **duplex** [full | half] **flowctrl** [enable | disable]

show port

- **port** { *port#* } - **設定を行うポートを指定。**
- **name** {*name*} - **ポート名を指定。**
- **admin** [enable | disable] - **ポートの有効 / 無効を指定。**
- **speed** [atuo | 10 | 100 | 1000] - **スピードを指定（**Autonegotiation,10M,100M,1000M**）**
- **duplex** [full | half] - **通信モードを指定。（全二重、半二重）**
- **flow** [enable | disable] - **フローコントロールの** ON/OFF
- **show port** - **ポートの設定情報および現在の接続情報を表示します。**

初期設定

（全ポート）

名前：10/100M base-T　　**有効 / 無効：有効**

通信速度・モード：オートネゴシエーション　　**フローコントロール：**OFF

例

ポート 1 **番の名前を** FXC_port1、speed/duplex **を** 100M Full、**フローコントロール** ON **にし、ポート** 2 **番を無効にします。その後、ポートの現在の設定および状況を表示します。**

```
10-port Intelligent Switch>set port 1 name fxc_port1 speed 100 duplex
full flow enable
Set port name successful!
Set port speed successful!
Set port duplex successful!
Set port flow successful!
10-port Intelligent Switch>show port
[Port Configuration]
Port Name         Status  Admin     AN   Speed   Duplex   Flow
  1  fxc_port1     DOWN    Enabled   OFF  100      Full     Enabled
  2  Port 2       DOWN    Enabled   ON   10      Half     Disabled
  3  Port 3       DOWN    Enabled   ON   10      Half     Disabled
  4  Port 4       DOWN    Enabled   ON   10      Half     Disabled
  5  Port 5       DOWN    Enabled   ON   10      Half     Disabled
  6  Port 6       DOWN    Enabled   ON   10      Half     Disabled
  7  Port 7       DOWN    Enabled   ON   10      Half     Disabled
  8  Port 8       DOWN    Enabled   ON   10      Half     Disabled
  9  Port 9       DOWN    Enabled   ON   1000    Full     Enabled
 10  Port 10      DOWN    Enabled   ON   10      Half     Enabled
```

qos ー Quality of Service

本機は、それぞれのポートで 2 **つのプライオリティキューをサポートしています。(**High/ Low**)。また、ポートベースおよび** 802.1p **をサポートしています。これらの機能は、スイッチの** High/Low **プライオリティキュー設定を行うために使用できます。**

"show qos" **コマンドで、現在の** QoS **の設定情報が表示できます。**

文法

set qos [enable ｜ disable]

set qos priority { *port#* } [high ｜ low]

set qos hq { *weight* }

set qos lq { *weight* }

set qos pt { *threshold* }

show qos

- **qos** [enable ｜ disable] - QoS **の有効** / **無効を指定**
- **priority** { *port#* } [high ｜ low] - **ポートベースの優先度を設定します。**
  - ー *port#* **:設定するポートを指定します。**
  - ー high ｜ low **:ポートの優先度を** high **または** low **に設定します。**
- **hq** { *weight* } - **高プライオリティキュートラフィックレートのウェイトを設定します。(**0-15**)**
- **lq** { *weight* } - **低プライオリティキュートラフィックレートのウェイトを設定します。(**0-15**)**
- **pt** { *threshold* } - 802.1P **タグパケットの高および低プライオリティキューの閾値を設定します。例えば** "set qos pt 4" **と設定をした場合、**4 **〜** 7 **のプライオリティ値の付いた** 802.1P **タグパケットは高プライオリティキューとなり、**0 **〜** 3 **は低プライオリティになります。(**0-7**)**
- **show qos** - QoS **の設定情報を表示します。**

初期設定

Qos setting：Disable　　802.1p Priority：0

Priority：　全ポート　Low

HQ Weight：4　　LQ Weight：1

例

QoS 機能を有効にし、ポート 3 番のプライオリティを High、ポート 4 番を Low、ポート 5 番および 6 番、7 番を High、高プライオリティのウェイトを 5、低プライオリティのウェイトを 3、802.1p 閾値を 2 に設定しています。その後に QoS の設定情報を表示しています。

```
10-port Intelligent Switch>set qos enable priority 3 high priority 4 low
priorit
y 5 high priority 6 high priority 7 high hq 5 lq 3 pt 2
Qos setting = Enabled
Set port priority successful!
Set port priority successful!
Set port priority successful!
Set port priority successful!
Set port priority successful!
Set HQ setting successful!
Set LQ setting successful!
Set 802.1p setting successful!
10-port Intelligent Switch>show qos
[QoS Configuration]
Qos setting    : Enabled
802.1p Priority: 2
HQ Weight      : 5
LQ Weight      : 3
Port  Priority  Port  Priority  Port  Priority  Port  Priority
[ 1]  Low       [ 2]  Low       [ 3]  Low       [ 4]  Low
[ 5]  High      [ 6]  High      [ 7]  High      [ 8]  Low
[ 9]  Low       [10]  Low
```

snmp ー SNMP（Simple Network Management Protocol）

本機の SNMP **機能を設定します。**

"show snmp" **で** SNMP **の現在の設定内容を表示します。**

文法

set snmp name { *name* }

set snmp location { *location* }

set snmp contact { *contact* }

set snmp getcommunity { *community name* }

set snmp setcommunity { *community name* }

set snmp trapcommunity { *index* } {*community name* }

set snmp trapip { *index* } { *trapip* }

set snmp txtrap { *index* }

show snmp

- **name** { *name* } - **本機の名称を指定します。**
- **location** { *location* } - **本機の設置場所を指定します。**
- **contact** { *contact* } - **本機にトラブルが発生した場合の連絡先を指定します。**
- **getcommunity** { *community name* } - Get **コミュニティ名を指定します。**
- **setcommunity** { *community name* } -Set **コミュニティ名を指定します。**
- **trapcommunity** { *index* } {*community name* }

  ー *index*：Trap **コミュニティ名を設定するインデックスを指定します。**

  ー *community name*：**指定したインデックスに** Trap **コミュニティを設定します。**
- **trapip** {*index*} {*trapip*} - 802.1p **の優先度**(0 〜 7)**を** 4 **つの優先度キューに割り当てます。**

  ー *index*：Trap **の送信先** IP **アドレスを設定するインデックスを指定します。**

  ー *trapip*：**指定したインデックスに** Trap **を送信する** IP **アドレスを設定します。**
- **txtrap** {*index*} - Trap **をテスト送信します。テスト送信をするインデックスを指定します。**

例

```
10-port Intelligent Switch>set snmp name ABC location AAA-1F
contact JACK
Set SNMP system name successful!
Set SNMP system location successful!
Set SNMP system contact name successful!
```

trunk ートランク

本機は、ポートベーストランクと MAC **ベーストランクをサポートしています。**

ポートベーストランクオペレーションは、物理的なポートアサイメントに基づいてトラフィックが割り当てられます。

MAC **ベーストランクオペレーションは、**MAC **アドレスに基づいてトラフィックがアサインされます。**

トランクグループは初期状態で無効かつ、作成されていません。本コマンドにてトランクの機能の設定をおこないます。

“show trunk“ **で、現在の設定情報が表示されます。**

文法

set trunk [enable | disable]

set trunk { + , - } { *port#* } { *trunk* }

set mactrunk [enable | disable]

set mactrunk { *port#* } { *trunk* }

set mactrunk hush [DA | SA | ALL]

set mactrunk giga [disable | 0]

ー disable**：ギガポートトランキングを無効にします。**

ー 0**：有効にするギガグループ** ID **を指定します。**0 **はポート** 9/G1**、ポート** 10/G2 **（本機では** "0" **のみ選択可能です）**

set trunkforward [auto | manual]

ー auto**：転送マップ割り当てを自動でおこないます。**

ー auto**：転送マップ割り当てを手動でおこないます。**

set trunkforward { + , - } { *port#* } { *trunk* }

show trunk

dell trunk { *trunk#* }

dell mactrunk { *trunk#* }

dell trunkforward { *Port#* }

- **trunk** { enable | disable} **- トランク機能の有効 / 無効を指定。**
- **trunk** { + , - } { *port#* } { *trunk* } **- 追加（または削除）したいポート番号を " ＋ " の後に入力。トランクから削除したいポートを " ー " の後に入力後、追加（または削除）をするトランク番号を指定します。**
- **mactrunk** [enable | disable] **-** MAC **ベーストランク機能の有効 / 無効を設定します。**
- **mactrunk** { *port#* } { *trunk* } **- 追加（または削除）したいポート番号を " ＋ " の後に入力。トランクから削除したいポートを " ー " の後に入力後、追加（または削除）をするトランク番号を指定します。**
- **mactrunk hush** [DA | SA | ALL]
- **show trunk - トランクの設定情報を表示します。**

ー DA**：インデックス生成に宛先アドレスを使用します。**

ー SA**：インデックス生成に送信元アドレスを使用します。**

– ALL：インデックス生成に宛先・送信元アドレス両方を使用します。

- **mactrunk giga** [disable | 0]
  – disable：ギガポートトランキングを無効にします。
  – 0：有効にするギガグループ ID を指定します。0 はポート 9/G1、ポート 10/G2（本機では "0" のみ選択可能です）
- **trunkforward** [auto | manual]
  – auto：転送マップ割り当てを自動でおこないます。
  – manual：転送マップ割り当てを手動でおこないます。
- **trunkforward** { + , - } { *port#* } { *trunk* } - 追加(または削除)したいポート番号を " ＋ " の後に入力。トランクから削除したいポートを " － " の後に入力後、追加（または削除）をするトランク番号を指定します。
- **dell trunk** {*trunk#*} - 指定したトランクグループを削除します。
- **dell mactrunk** { *trunk#* } - 指定した MAC トランクグループを削除します。
- **dell trunkforward** { *Port#* } - 指定したフォワーディングポートを、ポートベーストランクグループから削除します。
- **show trunk** - トランクの設定情報を表示します。

初期設定

Disable（無効）

例

トランクを有効にし、ポート 1,3,5 をトランク 3 に追加後、トランク 3 からポート 3 を削除します。

その後にトランク 3 を削除し、trunkforward を自動に設定します。

```
10-port Intelligent Switch>set trunk enable
Trunk Type: Port-based Trunk
10-port Intelligent Switch>set trunk +1+3+5 3
Port-based Trunk Group 3 setting:
[TRUNK]  [Port List]
=======  =======================================
 [ 3]     1  3  5
[Trunk Forward Setting]
[FWD]    [Port List]
=======  =======================================
 [ 1]
 [ 3]
 [ 5]
10-port Intelligent Switch>set trunk -3+7 3
Port-based Trunk Group 3 setting:
[TRUNK]  [Port List]
=======  =======================================
 [ 3]     1  5  7
[Trunk Forward Setting]
[FWD]    [Port List]
=======  =======================================
 [ 1]
 [ 5]
 [ 7]
10-port Intelligent Switch>del trunk 3
OK to destroy trunk group 3
10-port Intelligent Switch>set trunkforward auto
Trunk Forward  map is assigned by automatically
10-port Intelligent Switch>
```

例

MAC トランクを有効にし、トランク 2 にポート 3,5,7 を登録します。ハッシュインデックスを DA に設定、ギガポートトランキングを "o" にしています。

```
10-port Intelligent Switch>set mactrunk enable
Trunk Setting: MAC-based Trunk
10-port Intelligent Switch>set mactrunk +3+5+7 2
MAC-based Trunk Group 2 setting:
[TRUNK]  [Port List]
=======  =======================================
 [ 2]     3  5  7
10-port Intelligent Switch>set mactrunk hash da
Trunk Hash Index Selection: Destination Address
10-port Intelligent Switch>set mactrunk giga 0
Giga port trunking: Group 0
```

vlan-VLAN の設定

ポートベース VLAN の設定をおこないます。"show vlan" で現在の VLAN テーブルを表示します。

文法

set vlan [*enable* | *disable*]

set vlan [+| -]{ *Port#* } { *vlan#* }

show vlan

- **set vlan** [*enable* | *disable*] -VLAN 機能の有効 / 無効を設定します。
- **set vlan** [+| -]{ *Port#* } { *vlan#* } - ポート番号の前に " ＋ " を付けると、指定した VLAN へポートを追加します。" - " を付けると VLAN からポートを削除します。
- **show vlan** - 現在の VLAN テーブルを表示します。

初期設定

なし

例

VLAN を有効にし、VLAN 3 にポート 5 を追加、VLAN5 にポート 7.8 を追加後、VLAN5 からポート 7 を削除。その後に VLAN テーブルを表示しています。

```
10-port Intelligent Switch>set vlan enable
VLAN Setting:  Enabled
10-port Intelligent Switch>set vlan +5 3
VLAN 3 setting:
[VLAN]   [Port List]
======   =======================================
 [ 3]    5
10-port Intelligent Switch>set vlan +7 5
VLAN 5 setting:
[VLAN]   [Port List]
======   =======================================
 [ 5]    7
10-port Intelligent Switch>set vlan +8 5
VLAN 5 setting:
[VLAN]   [Port List]
======   =======================================
 [ 5]    7  8
10-port Intelligent Switch>set vlan -7 5
VLAN 5 setting:
[VLAN]   [Port List]
======   =======================================
 [ 5]    8
10-port Intelligent Switch>show vlan
VLAN Setting:  Enabled

[VLAN]   [Port List]
======   =======================================
 [ 3]    5
 [ 5]    8
```

1qvlan ー 802.1QVLAN

このコマンドは 802.1QVLAN **の設定を行います。**
"show 1qvlan" **で、現在の設定情報が表示されます。**

文法

set 1qvlan [enable **|** disable]

set 1qvlan membermap vid {*VID#* } [+ **|** -]{ *Port#* }

set 1qvlan tag vid {*VID#* } [+ **|** -]{ *Port#* }

set 1qvlan default_tag port { *Port#* } **pvid** {*pvid#* } **pri** {*pri#* }

set 1qvlan newprimap [enable **|** disable] [oldpri-newpri]

set 1qvlan frame_cntl [none **|** vid **|** priority **|** vid_priority]

set 1qvlan vtable [drop **|** flood]

set 1qvlan ifilter [on **|** off]

set 1qvlan drop_n_1q port { *Port#* } [drop **|** nondrop]

show 1qvlan

- **1qvlan** [enable **|** disable] -1QVLAN **の有効** / **無効を設定します。**
- **membermap** -1QVLAN **テーブルメンバーシップを設定します。**VID(1-4094)**を指定し、ポートの追加(前に** " ＋ " **を付ける)、削除(前に** "-" **を付ける)を行います。**
- **tag** - 1QVLAN **テーブルポートのタグ付き** / **タグ無しを設定します。**VID(1-4094)**を指定し、タグ付き(前に** " ＋ " **を付ける)、タグ無し(前に** "-" **を付ける)を設定します。**
- **default_tag** - **タグ付きポートの** VLAN ID **およびプライオリティを設定します。**
  - ー **port** { *Port#* } **:ポート番号を指定。**
  - ー **pvid** {*pvid#* }**:**PVID**(**1-4094**)**
  - ー **pri** {*pri#* } **:プライオリティを設定(**0-7**)**
- **newprimap** - **タグ機能の新しいプライオリティマッピングを行います。**
  - ー [enable **|** disable]**:有効:無効を設定します。**
  - ー oldpri-newpri**:旧プライオリティ(**0-7**)ー新プライオリティ(**0-7**)**
- **frame_cntl** - VLAN ID **およびプライオリティ値の再アサインを設定します。**
  - ー none**:変更無し。**
  - ー vid**:** VLAN ID **を変更。**
  - ー priority**:プライオリティを変更。**
  - ー vid_priority**:** vid_priority **に設定。**

[注意] "vtable" が "drop" または "ifilter" が "on" に設定されている場合、違う VLAN ID を持つパケットは最初に破棄されてしまうので VLAN ID の変更は行われません。

- **vtable -** **未知の** VLAN ID **のタグ**（VLAN **テーブルに載っていない** VLAN）**の付いたパケットの処置方法を設定します。**
  - drop：**パケットを破棄します。**
  - flood：**パケットを全てのポートへフラッティングします。**
- **ifilter -** **イングレスフィルタリングの** ON/OFF **を設定します。**
- **drop_n_1q -** **タグ無し**（802.1Q **以外**）**パケットの処置を設定します。**
  - drop：**パケットを破棄します。**
  - nondrop：**パケットを破棄せずフォワーディングをおこないます。**
- **show 1qvlan -** 1QVLAN **の設定情報を表示します。**

初期設定

802.1Q setting：Disabled　Frame Control：No change

Ingress filter：Filter Off　Vtable not found：Flood　Remap New Priority：Disabled

例

1QVLAN **を有効にし、**VID2 **にポート** 3、VID3 **にポート** 4、VID4 **もポート** 5 **を追加した後、**VID4 **のポートをタグ無しに設定しています。その後、デフォルトタグ設定を、ポート** 6 **の** PVID10 **プライオリティ** 6 **にしています。**

```
10-port Intelligent Switch>set 1qvlan enable
802.1Q setting = Enabled
10-port Intelligent Switch>set 1qvlan membermap vid 2 +3
[VID]   [Port List]
======  ========================================
 2        3[T]
10-port Intelligent Switch>set 1qvlan membermap vid 3 +4
[VID]   [Port List]
======  ========================================
 3        4[T]
10-port Intelligent Switch>set 1qvlan membermap vid 4 +5
[VID]   [Port List]
======  ========================================
 4        5[T]
10-port Intelligent Switch>set 1qvlan tag vid 4 -5
[VID]   [Port List]
======  ========================================
 4        5[U]
10-port Intelligent Switch>set 1qvlan default_tag port 6 pvid 10 pri 6
Port 6 Default untag priority=6, vid=10
```

dot1x ー 802.1X

802.1X **機能の設定を行います。**

“show dot1x“ **コマンドを使用して、現在の設定内容を確認できます。**

文法

set dot1x [*enable* | *disable*] **transparent re_au** [0:disable | 1:enable] **reauthtime** {*count*} **reauthcnt** {*count*} **reqcnt** {*count*} **sertime** {*period*} **supptime** {*period*} **quitetime** {*period*} **txtime** {*period*} **rsip** *{IP Address}* **authport** {*port#*} **shkey** {*key*} **portauth** {*mode*}

show dot1x [*config* | *radius* | *port*]

- **set dot1x** [*enable* | *disable*] - 802.1X **の有効 / 無効を設定します。**
- **transparent** - **トランスピアレントモードに設定します。**
- **re_au** [0:disable | 1:enable] - 802.1X **再認証を設定します。**
- **reauthtime** { *period* } - 802.1X **再認証タイムアウトの間隔を設定します。**
- **reauthcnt** { *count* } - 802.1X **再認証の回数を設定します。**
- **reqcnt** { *count* } - 802.1X **リクエストタイムの最大回数を設定します。**
- **sertime** { *period* } - **スイッチと** RADIUS **サーバ間のリクエストタイムアウト値を設定します。**
- **supptime** { *period* } - **スイッチとユーザ間のタイムアウト値を設定します。**
- **quiettime** { *period* } - **スイッチとユーザ間で、認証に失敗した際、次の認証プロセスまでの待ち時間を設定します。**
- **txtime** { *period* } - **スイッチからユーザへの認証リクエストのタイムアウト値を設定します。**
- **rsip** { *IP Address* } - RADIUS **サーバの** IP **アドレスを設定します。**
- **authport** { *port#* } - **認証ポートを設定します。**
- **shkey** { *key* } - **スイッチと** RADIUS **サーバ間のセキュリティキーを設定します。**
- **portauth** { *mode* } - **物理ポートの認証モードを設定します。**
  - **auto** **：ポートの認証結果に基づきます。**
  - **fa** **（**Force-authenticated**）：ポートは常に認証状態になります。**802.1X **プロセスの結果は無視されます。**
  - **fu** **（**Force-unauthenticated**）：ポートは常に非認証状態になります。**802.1X **プロセスの結果は無視されます。**
  - **non** **：**802.1X **無効。**

- **show dot1x** [*config* | *radius* | *port*] -802.1X **の設定情報を表示します。**

  - ー *config* ：802.1X **現在の設定内容を表示します。**
  - ー *radius* ：RADIUS **サーバに関する設定を表示します。**
  - ー *port* ：**ポート設定を表示します。**

初期設定

802.1x Protocol ：Disabled Re-authentication ：Disabled
Re-authentication Timeout Period ：3600 Re-authentication Max Count ：2
Max Request Count ：2 Server Timeout Period ：30
Supplicant Timeout Period ：30 Quiet Timeout Period ：60
Tx Timeout Period ：30 Redius Server IP Address ：192.168.1.222
Redius Server Port Number ：1812 Security Key ：12345678

例

802.1X **を有効にし、**re_au **を** 3、RADIUS **サーバ** IP **アドレスを** 192.168.1.5 **に設定しています。**

```
10-port Intelligent Switch>set dot1x enable transparent re_au 1
txtime 3 rsip 19
2.168.1.5
Enable 802.1x successful!
Enable 802.1x re-authenticate function!
Set transparent time successful!
Set IP address of Radius server successful!
```

※**本機は** MD5、TLS **および** PEAP **の認証方式をサポートしています。**

security ーセキュリティ

arl コマンドにて、登録した MAC アドレスを基に、アクセス制御を設定します。

“show security“ コマンドを使用して、現在の設定内容を確認できます。

文法

set security [enable | disable]

set security port { *Port#* } [no | accept]

show security

- [enable | disable] - セキュリティ機能の有効 / 無効を設定します。

[注意] 本機能と 802.1x 機能は同時に動作させせることができません。

- **port** { *Port#* } [no | accept]- ポートを番号を指定し、拒否または許可を選択します。
  - ー no ：ポートでセキュリティ機能を無効にします。
  - ー accept ：静的 MAC アドレスだけを許可するように設定します。ポート 1 にたいし、ポート 1 で構成を設定された静的な MAC アドレスを持つユーザのみを許可します。（学習されている MAC アドレスは arl ー ARL テーブル（P8）コマンドで確認ができます）
    MAC アドレスフィルターイン機能が動作するためには、以下の 2 つの条件が満たされる必要があります。
    1. ポートのセキュリティモードが "Accept" に設定されている。
    2. 静的 MAC アドレスがポートにアサインされている。
       （例：ポート 1 に MAC アドレス 1 がアサイン)
    この場合、MAC アドレス 1 のみがポート１を通ってネットワークへアクセスすることができます。
- **show security** - セキュリティの詳細情報を表示します。

初期設定

なし

関連する項目

arl ー ARL テーブル（P8）

例

セキュリティ機能を有効にし、ポート 3,5,7 **番を** "accept" **に設定後、**"show security" **にて現在の設定情報を表示しています。**

```
10-port Intelligent Switch>set security enable
Enable MAC Security successful!
10-port Intelligent Switch>set security port 3 accept
Set port mode successful!
10-port Intelligent Switch>set security port 5 accept
Set port mode successful!
10-port Intelligent Switch>set security port 7 accept
Set port mode successful!
10-port Intelligent Switch>show security
[MAC Security Configuration]
 MAC Security Setting : Enabled
================================================
  Port              Security Control
================================================
    1                  No Security
    2                  No Security
    3         Static mode with Accept function
    4                  No Security
    5         Static mode with Accept function
    6                  No Security
    7         Static mode with Accept function
    8                  No Security
    9                  No Security
   10                  No Security
================================================
```

sta ースパニングツリープロトコル

本機でスパニングツリープロトコルの設定を行います。本機は STP（802.1d）と互換性のある RSTP（802.1w）を使用することができます。

“show sta“ で、現在の設定情報が表示されます。

文法

set sta [enable **|** disable]

set sta bridge priority { *priority* } **hellp** { *hello time* } **age** { *maximum age* } **delay** { *delay time* }

set sta port { *port#* } **cost** { *cost* } **priority** { *priority* }

show sta

- **set sta** [enable | disable] - スイッチのスパニングツリー機能有効 / 無効を設定します。
- **sta bridge**
  - ー **priority** { *priority* } ：ルートデバイス、ルートポート、指定ポートを選択するために必要なブリッジプライオリティを設定します（0-65535）。最も高いプライオリティ（priority が最も低い）を持つデバイスはスパニングツリープロトコルのルートデバイスになります。すべてのデバイスが同じプライオリティの場合、最も低い MAC アドレスを持つデバイスがルートデバイスになります。
  - ー **hello** { *hello time* } ：本機がスパニングツリーのルートデバイスの場合に、スパニングツリー管理パケットを送信する間隔を設定します。（0-65535）
  - ー **age** { *maximum age* } ：スパニングツリー管理パケットを受信していない場合のスパニングツリーのエージングタイムを設定します。これはスパニングツリーの再作成を引き起こします。初期状態では 20 秒です。（6-40）
  - ー **delay** { *delay time* } ：スパニングツリーの状態を変更（リスニング状態からラーニング状態への移行）する前の最大待ち時間を設定します。この設定が必要とされるのは、すべてのデバイスがフレームの転送を始める前にトポロジの変更についての情報を受信する必要があるからです。加えて、各ポートはブロッキング状態に再び戻るような衝突情報（一時的なデータループの発生など）を検知するための時間が必要です。（4-30）
- **sta port**
  - ー { *port#* } ：ポート番号を指定します。
  - ー **cost** { *cost* }：ループが発生した場合にデバイス間の最適経路を決定するためにこの値が使用されます。速度が速いポートには低い値が割り当てられ、パケットの転送が行われます。速度が遅いポートには高い値が割り当てられ、転送がブロックされます。推奨される値は 10M で 100（50 ～ 600 の範囲）、100M で 19（10 ～ 60）、1000M で 4（3 ～ 10）です。
  - ー **priority** { *priority*} ：ポートのプライオリティを設定します。スイッチ上のすべてのポートのパスコストが同じの場合、ループが発生したときに最も高いプライオリティ（priority が最も低い）のポートに転送されます。最も高いプライオリティのポートが複数ある場合、最も低いポート番号のポートに転送されます。（0-255）
- **show sta -** スパニングツリーの設定情報を表示します。

初期設定

STA：Disabled　Bridge Priority ：32768　Bridge Hello Time ：2

Bridge Max Age：20　Bridge Forward Delay :：15　Port Priority：128

例

スイッチで STA を有効にし、ブリッジの設定を行います。その後にポート 3 を指定して、有効にした後、コスト / プライオリティの設定を行います。

```
10-port Intelligent Switch>set sta enable
Enable Spanning Tree function successful!
10-port Intelligent Switch>set sta bridge priority 100 hello 2
age 20 delay 30
Set priority successful!
Set hello time successful!
Set max age successful!
Set forward delay successful!
10-port Intelligent Switch>set sta port 5 cost 19 priority 100
Port 5 path cost = 19
Port 5 priority = 100
```

http ー HTTP アクセス

本機の HTTP **を通した設定機能を有効・無効に設定します。ハッカーやワーム・ウイルスが頻繁に** HTTP **サーバーを攻撃しているならば、このコマンドで** HTTP **機能を無効にしてください。**

"show http" **で、現在の設定情報が表示されます。**

[注意]　本機がファイアーウォール等の防御を行わずにインターネット環境下に接続されている場合、本機能で HTTP を無効にし、Telnet または SNMP からの管理を行うことを推奨します。

文法

set http [enable | disable]

show http

- enable | disable - HTTP **機能の有効 / 無効を設定します。**
- **show http** - http **設定情報を表示します。**

[注意]　“set http“ コマンド実行後、本機は自動的に再起動されます。

初期設定

Enable**（有効）**

例

HTTP **機能を無効に設定しています。**

```
10-port Intelligent Switch>set http disable
Disable http function successful!
Reset system ......
10-port Intelligent Switch>+
Booting Program Version 1.02.00, built at 08:42:45, Mar 30 2004

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05900000, 16 blocks of 0x00010000 bytes
each.
==> enter ^C to abort booting within 3 seconds ......

Start to run system initialization task.
[System Configuration]
Company Name      :
Model Name        : 10-port Intelligent Switch
MAC  Address      : 00:C0:F6:63:01:5E

Firmware version: 2.20.14 (built at Sep 19 2005 10:34:25)
Press <ENTER> key to start.
UCD-SNMP version 4.1.2

Username:admin
Password:
```

show cfg －機器情報の表示

本機のモデルネーム、MAC **アドレスを表示します。**

文法

show cfg

例

```
10-port Intelligent Switch>show cfg
[System Configuration]
Model   Name : 10-port Intelligent Switch
MAC  Address : 00:C0:F6:63:01:5E
```

show version －ファームウェアバージョンの表示

ファームウェアバージョンを表示します。

文法

show version

例

```
10-port Intelligent Switch>show version
Firmware Version: 2.20.14 (built at Sep 19 2005 10:34:25)
```

upgrade －アップグレード

TFTP **サーバ経由で、ソフトウェア（ファームウェアまたはコンフィグレーション）のアップグレードを行います。**

文法

upgrade [firmware | config] {*ip address* } { *filename* }

- [firmware | config] - **ファームウェアまたはコンフィグレーションを選択します。**
- *ip address* - TFTP **サーバの** IP **アドレスを指定します。**
- *filename* - **アップグレードファイル名を指定します。**

例

```
10-port Intelligent Switch>upgrade config 192.168.1.7 3009_1123.cfg
Download the header of configuration file......OK.
Verify header of configuration firmware......OK.
Start to download configuration file......OK.
Verify configuration file......OK.
Erase configuration file......OK.
Programming configuration file......OK.
Restart system......
```

関連する項目

backup **－バックアップ（**P5**）**

2. Web インタフェースからの設定

2.1 Web インターフェースへの接続

本機には管理用の Web サーバが搭載されています。Web ブラウザから設定を行うことができます。

Web インターフェースを使用する場合には、事前に以下の設定を行ってください。

(1) コンソール接続を使用し、本機に IP アドレス、サブネットマスク、デフォルトゲートウェイを設定します。(詳細は P9 「eth0 − IP 設定」を参照して下さい)

(2) コンソール接続で、ユーザー名とパスワードを設定します。Web インタフェースへの接続はコンソール接続の場合と同じユーザー名とパスワード使用します。

(3) Web ブラウザから、設定した IP アドレスに接続し、ユーザー名とパスワードを入力すると、アクセスが許可され、本機のホームページが表示されます。

Web サーバーへのアクセスが確立されると、以下の画面が表示されます。

- Link Up
- Link Down
- Port Disable

10-port Intelligent Switch
2.20.14 (built at Sep 19 2005 10:34:25)

System Configuration
Port Configuration
Spanning Tree
Static Address Table
Address Table
MAC Security Configuration
802.1Q Virtual LAN
802.1Q VLAN Table
Port-Based Virtual LAN
Mirror
QoS
SNMP
Trunk
IGMP
802.1x Configuration

System Configuration

Main Board Information	
Firmware Version	2.20.14 (built at Sep 19 2005 10:34:25)
Mac Address	00:C0:F6:63:01:5E
Number of Ports	10
IGMP Max. Group	256
1Q VLAN Max. Group	512
Auto Mode	Auto Detect / Auto Negotiation
ARL Aging	Enable / Disable
ARL Aging Time (seconds)	300
	Apply

Network Configuration	
IP Address	192.168.1.5
Network Mask	255.255.255.0
Gateway	192.168.1.1

2.2 Web インターフェースの操作方法

2.2.1 パネルの表示

Web インタフェースではポートの状態が画像で表示されます。各ポートのリンク状態を確認することができます。また、各ポートをクリックすることで各ポートの設定ページが表示されます。



Port Summary

Port state summary							
Port Number	Type	Link Status	Admin Status	Auto. Negotiation	Speed Status	Duplex Status	Flow Control
7	100TX	Up	Enable	Enable	100Mbps	Full	Disable

Port Statistics			
In Octets	229129	Out Octets	1246915
In Unicast Pkts.	1737	Out Unicast Pkts.	1724
In Non-Unicast Pkts.	178	Out Non-Unicast Pkts.	0
In Discards	0	Out Discards	0
In Errors	0	Out Errors	0
Alignment Errors	0	CRC Errors	0
Single Collisions	0	Multiples Collisions	0
Defered Transmissions	0	Late Collisions	0
Excess Collisions	0	Carrier Sense Errors	0
Drop Events	0	Fragments	0
Octets	229129	Jabbers	0

Apply Refresh

2.2.2 設定

ページ上で設定変更を行った際は、必ず新しい設定を反映させるために [Apply] ボタン（または [Create]、[Delete] ボタン）を押してください。

1 ページ内の各項目ごとに [Apply] ボタンが設置されている場合は、必ず各設定を行うごとにその項目に対応する [Apply] ボタンを押してください。

2.3 システム設定

System Configuration

Main Board Information	
Firmware Version	2.20.14 (built at Sep 19 2005 10:34:25)
Mac Address	00:C0:F6:63:01:5E
Number of Ports	10
IGMP Max. Group	256
1Q VLAN Max. Group	512
Auto Mode	◉ Auto Detect ○ Auto Negotiation
ARL Aging	◉ Enable ○ Disable
ARL Aging Time (seconds)	300
	Apply

Network Configuration	
IP Address	192.168.1.5
Network Mask	255.255.255.0
Gateway	192.168.1.1
	Apply

Administrator Configuration	
Old Username	
Old Password	
New Username	
New Password	
Confirm Password	
	Apply

ファンクションリストから "System Configuration" を選択します。
本機の基本情報（ファームウェアバージョン、MAC アドレス等）を確認できます。

ネットワーク設定等もこのページで行えます。

Auto Mode

- Auto Detect - 対向の機器のオートネゴシエーション機能が有効の場合は ad mode を選択します。
- Auto Negotiation - 対向の機器のオートネゴシエーション機能が無効になっている場合は an mode を選択します。

どちらのモードを選択するかは、各ネットワーク構成によって異なります。
ほとんどのケースでは ad モードが推奨されています。

ARL Aging

- Enable - ARL テーブルエージングタイムを有効にします。
- Disable- ARL エージングタイムを無効にします。

ARL Aging Time (seconds)

ARL テーブルがクリアされるまでの秒数を設定します。（初期設定値：300 秒）

Network Configuration

本機の IP アドレス、ネットワークマスク、デフォルトゲートウェイの設定を行います。

Administrator Configuration

ネットワーク管理者の、ユーザ名 / パスワードを変更できます。（初期設定：admin/123456）

[Apply] をクリックすることで新しい設定が適用されます。

2.4 ポート設定

Port Configuration

Port#	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	
1	Enable	Enable	10M Half	Disable	Apply

Current Setting & Link Status

Port#	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	Link Status
1	Enable	Enable	10M Half	Disable	Down
2	Enable	Enable	10M Half	Disable	Down
3	Enable	Enable	10M Half	Disable	Down
4	Enable	Enable	10M Half	Disable	Down
5	Enable	Enable	10M Half	Disable	Down
6	Enable	Enable	10M Half	Disable	Down
7	Enable	Enable	100M Full	Disable	Up
8	Enable	Enable	10M Half	Disable	Down
9	Enable	Enable	1000M Full	Enable	Down
10	Enable	Enable	10M Half	Enable	Down

ファンクションリストから "Port Configuration" を選択します。

上段の ”Port Configuration” で、選択したポートごとの各種設定を行います。

下段の ”Current Setting&Link Status” では、設定情報及び、ポートのリンク状態を確認できます。

Port Configuration（ポート設定）

（1）設定を行うポートを選択します。

（2）"Admin" の Enable（有効）/ Disable（無効）を選択します。"disable" に設定した場合、このポートでは全てのネットワークアクセスが無効になります。

（3）ポートのオート機能の Enable（有効）/ Disable（無効）を設定します。オートモードは P35 「システム設定」にて ”auto-negotiation” または ”auto-detect” から選択をすることができます。

（4）オートモードが無効の場合、”Speed”、”Duplex” にて、速度と duplex モードを設定します。

（5）フローコントロール機能の Enable（有効）/ Disable（無効）を設定します。（フローコントロールは、フローコントロール設定および QoS の両方で "ON" になっている場合に動作します）

（6）[Apply] をクリックします。

2.5 スパニングツリー

Spanning Tree -- Bridge

Bridge Configuration	
Spanning Tree	○ Enable ◉ Disable
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Maximun Age	20
Apply	
Configuration STA Port	

スパニングツリープロトコルの設定を行います。
ファンクションリストより "Spanning Tree" を選択します。
パラメータについては P28 「sta ースパニングツリープロトコル」を参照してください。
変更後は [Apply] をクリックしてください。
スパニングツリーのポート設定は "Configuration STA Port" で行います。

Spanning Tree -- Bridge Port

Bridge Port Number	1
Port Priority (0..255)	128
Port State	None
Port Enable	◉ Enable ○ Disable
Port Path Cost (1..65535)	19
Port Designated Root	00:00:00:00:00:00 [0]
Port Designated Cost	0
Port Designated Bridge	00:00:00:00:00:00 [0]
Designated Port	0: [0]
Port Forward Transitions	0
Apply	
Configure STA Bridge	

関連する項目

sta ースパニングツリープロトコル（P28）

2.6　MAC アドレステーブル

2.6.1　静的アドレステーブル

Static Address Table

Entry ID	Add New Entry
Priority	Low　High
MAC Address (XX-XX-XX-XX-XX-XX)	
Destination Port	1 2 3 4 5 6 7 8 9 10
Confirm Add/Change	

Current Static Address Setting

ID	VID	Priority	MAC Address	Destination Port		
1		High	33-55-66-77-88-c0	3	Edit	Delete

本機はスタティック MAC アドレスの割り当てをサポートしています。本機はこれらのスタティック MAC アドレスをエージアウトしません。

ポートセキュリティ機能について

MAC アドレスを使ったポートのセキュリティ機能を "MAC Security Configuration" のページで設定することができます。Accept モードではスタティック MAC アドレスのみ、ポートを通してネットワークにアクセスできます。

学習された MAC アドレスはアドレステーブルページの、それぞれのポートで確認できます。

スタティック MAC アドレステーブルのエントリを削除したい場合、エントリの "Delete" ボタンをクリックしてスタティック MAC アドレスをテーブルから取り除いてください。

関連する項目

Mac セキュリティ（P41）

2.6.2 アドレステーブル

Address Table

Total Pages : 1 [Previous Page] [Next Page] Go to Page : Current Pages : 1

ID	MAC Address	VID	Priority	Destination Port	Status
1	00-13-d3-ed-cb-67		Low	7	Dynamic

このページでは本機で学習された MAC アドレステーブルを表示します。

[注意] スイッチがエージングタイムの動作を行っていると、不正な MAC アドレスが MAC アドレステーブルに時々発見されます。これらの不正な MAC アドレスはこれまでにポートにアクセスしたことのある機器であり、スイッチがそれらをテーブル内に学習しています。スイッチはエージングタイムが終わったとき、その MAC アドレスを消去します。ユーザーは正しい MAC アドレステーブルを得たいとき、エージングタイムを短くし Web ブラウザを再読み込みすることができます。正確な MAC アドレステーブルを得たとき、エージングタイムから回復します。

2.7 Mac セキュリティ

MAC Security Configuration

MAC Security	○ Enable ⦿ Disable	Apply

Port Number	Security Control
1	No Security
2	No Security
3	No Security
4	No Security
5	No Security
6	No Security
7	No Security
8	No Security
9	No Security
10	No Security

Apply

このページではポート上に設定したスタティック MAC アドレスのセキュリティモードを設定するために使用します。

– No Security
ポートにアクセスの制限を行いません。MAC アドレスを持つすべての機器がポートを通してネットワークにアクセスできます。

– Accept function
スタティック MAC アドレスとして設定されている機器のみポートを通してネットワークにアクセスできます。

設定手順

（1）あらかじめ、802.1x 機能を無効にします。

（2）MAC セキュリティを有効にします。

（3）ポートの "Security Control" を "Accept function" に設定します。

（4）スタティック MAC アドレスとして設定されている機器のみがポートを通してネットワークにアクセスできます。（スイッチが学習している MAC アドレスは Address Table ページで確認できます)

関連する項目

静的アドレステーブル（P39）

2.8 VLAN

2.8.1 802.1Q VLAN 設定

802.1Q Virtual LAN

VLAN	⊙ Disable ○ 802.1Q VLAN ○ Port-Based VLAN	Apply

Frame Control

802.1Q Frame Control	Ingress Filter	Vtable not found
No Change	Filter OFF	Flood

Not 1Q Frame Control

Port#	1	2	3	4	5	6	7	8
No Drop	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
Drop	○	○	○	○	○	○	○	○

New Priority Map : ⊙Disabled ○Enable

Old Priority Map	0	1	2	3	4	5	6	7
New Priority Map	0	0	0	0	0	0	0	0

Apply

Default Tag Setting

Port#	1	2	3	4	5	6	7	8	9	10
PVID	1	1	1	1	1	1	1	1	1	1
Priority	0	0	0	0	0	0	0	0	0	0

Management Port : PVID : 1 Priority : 0

Apply

このページでは 802.1Q VLAN 機能の設定を行います。

802.1QVLAN のオペレーションはパケットの「タグ」に基づいています。
タグは 12 ビットの VLAN ID と 3 ビットのプライオリティ情報を含んでいます。

tagged ポートから送られたパケットは常にタグ付きパケットとなり、untag ポートから送られたパケットは常にタグ無しパケットとなります。

それぞれの物理ポートにデフォルトタグ設定を割り当てることができ、デフォルト設定には、VLAN ID およびポートのプライオリティを含みます。
タグポートにて、タグ無しパケットが受信、転送される場合、デフォルト設定がタグに付加されます。

設定・表示項目

VLAN

“Disable“ “Port-based VLAN“ “802.1QVLAN“ を選択します。

802.1Q Frame Control

パケットの、VLAN ID およびプライオリティの設定を変更することができます。

“No Change“ “Change Priority“ “Change VID“ “Change Both“ から選択をします。

修正の必要がある場合、デフォルトタグ値はパケットの VLAN ID またはプライオリティに置き換えられます。

[注意] "Ingress Filter" が "ON" または "Vtable not found" が "Drop" に設定されている場合、異なる VLAN ID を持つパケットは最初に破棄されるので、VLAN ID 修正の効果はありません。

Ingress Filter

イングレスフィルタ機能はポートの入力側で VLAN のフィルタを行います。ポートが受信した VLAN がポートに設定した VLAN と同一の場合、出力ポートに転送します。それ以外は破棄します。

Vtable not found

未知の VLAN ID（スイッチの VLAN テーブルに学習されていない）を持つパケットを破棄または、全てのポートにフラッティングすることができます。

Not 1Q Frame Control

タグ無しパケットが受信された場合に、破棄もしくは転送を選択することができます。

New Priority Map

プライオリティオペレーションの再マッピングが可能です。
例えば、プライオリティ 3 をプライオリティ 5 にマップすることで、全てのプライオリティ 3 を持つパケットを、プライオリティ 5 を持つパケットとして扱うことができます。

VID and Priority for Port 1~10

それぞれの物理ポートのデフォルトタグ設定です。
これらの値はタグの不可およびフレーム制御に使用されます。

VID and Priority for Management Port

ここでは本機の管理用インターフェースの PVID を指定することができます。
HTTP、Telnet、SNMP によるネットワーク経由でのスイッチの管理ができるユーザーが、Management Port の PVID を持つ VID の VLAN のユーザーに限定されます。

2.8.2 802.1Q VLAN テーブル

802.1Q VLAN Table

VLAN MemberShip Setting

VID : [ ] Select

VID	Name	1	2	3	4	5	6	7	8	9	10

Confirm Add/Change　Delete

Active VID Table

Total page : 1　Current page : 1　Go to page : [ ] Apply　Previous Page　Next Page

VID	Name	1	2	3	4	5	6	7	8	9	10
1	Default	U	U	U	U	U	U	U	U	U	U

設定・表示項目

802.1Q VLAN Table

設定手順は以下です。

（1）“VID“ に VLAN ID を入力し [Select] をクリックします。

（2）"Name" に VLAN 名を入力します。

（3）追加するポートにチェックを入れ（VLAN から削除したいポートはチェックを外す）ます。"T" はタグ付き、"U" はタグ無しです。ブランクは VLAN メンバーではないことを表します。

（4）“Confirm Add/Change” をクリックし、設定を完了します。

Acctive VID Table

802.1QVLAN の設定を表示します。

2.8.3　ポートベース VLAN

Port-Based Virtual LAN

VLAN　◉ Disable　○ 802.1Q VLAN　○ Port-Based VLAN　[Apply]

VLAN	Name	1	2	3	4	5	6	7	8	9	10
1		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

[Apply]

設定・表示項目

ポートベース VLAN **の設定を行います。**

設定手順は以下です。

（1）“VLAN” **で、**“Port-Based VLAN“ **を選択します。**

（2）VLAN **名を入力します。**

（3）VLAN **メンバーポートにチェックを入れます。**

（4）[Apply] **をクリックします。**

2.9 ポートミラーリング

Mirror

Mirroring	○ Enable ◉ Disable

Port Number	1	2	3	4	5	6	7	8	9	10
Capture Port	◉	○	○	○	○	○	○	○	○	○

Ingress

Port Number	1	2	3	4	5	6	7	8	9	10
Monitored Port(s)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Filter Mode	◉ All Packets ○ DA ○ SA									
Capture Frequency	Mirror one of 1 Packets.									

Egress

Port Number	1	2	3	4	5	6	7	8	9	10
Monitored Port(s)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Filter Mode	◉ All Packets ○ DA ○ SA									
Capture Frequency	Mirror one of 1 Packets.									

Apply

設定・表示項目

ポートミラーリングの機能を設定するには下記の手順を実行します。

(5) ポートミラーリングを有効にします。

(6) “Capture Port”（パケットをミラーするポート）を選択します。

(7) 監視したいトラフィックの向き（ポートの入力方面、出力方面）により、Ingress か Egress のテーブルからモニターポートを選択します。

(8) キャプチャ方式（Filter Mode）を選択します。

- ALL Packets
  すべてのパケットをキャプチャします。
- IDA
  受信したパケットの送信先 MAC アドレスに一致するパケットのみキャプチャします。
- ISA
  受信したパケットの送信元 MAC アドレスに一致するパケットのみキャプチャします。

(9) キャプチャしたパケットのうちミラーポートに送信する割合を選択します。初期状態ではキャプチャしたすべてのパケットをミラーポートに送信します。例えば 2 を設定するとキャプチャしたパケット 2 個のうち 1 個が、4 を設定するとキャプチャしたパケット 4 個のうち 1 個がミラーポートに送信されます。

(10) [Apply] をクリックします。

ポートミラーリングを無効にしたい場合、”Disable” を選択して [Apply] をクリックしてください。

2.10 QoS

QoS

QoS	○ Enable ⊙ Disable

Port Priority

Port#	1	2	3	4	5	6	7	8	9	10
High	○	○	○	○	○	○	○	○	○	○
Low	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙

Priority Queue Weighting

Weights of High-Priority Queue (1 - 15)	4	Weights of Low-Priority Queue (1 - 15)	1

802.1P Priority to Priority Queue

Threshold for 802.1P (0 - 7)	0

Apply

設定・表示項目

本機の QoS 機能は、それぞれのポートで 2 段階のプライオリティキューをサポートしています。

（1）まず QoS を "Enable" にします。

（2）ポートベースの優先度を使用する場合、ポートに High もしくは Low の優先度を設定します。

（3）High プライオリティおよび Low プライオリティに、トラフィックレートのウェイトを設定します。

（4）802.1p の優先度を使用する場合、プライオリティ値は 0~7 になります。High プライオリティキューへ、プライオリティ値の閾値を設定します。

（5）[Apply] をクリックし、設定を適用します。
QoS の動作を無効にしたい場合、Disable を選択して [Apply] をクリックします

関連する項目

qos ー Quality of Service（P15）

2.11 SNMP

System Information

Object ID :	1.3.6.1.4.1.655.6.5
Up Time :	0 day 1 hour 18 min 32 sec
Name :	
Contact :	
Location :	

SNMP -- Communities

	Community Name
GET	public
SET	private

SNMP -- IP Trap Manager

IP Address	Community Name	Status
0.0.0.0	public	Disable
0.0.0.0	public	Disable
0.0.0.0	public	Disable
0.0.0.0	public	Disable
0.0.0.0	public	Disable

Apply

このページでは GET/SET/Trap のコミュニティ名、Trap の動作のための IP アドレスを設定することができます。設定を行うと、SNMP の管理プログラムからこれらの設定を使用して本機を管理することができます。

2.12 トランク

本機は、ポートベーストランクと MAC ベーストランクをサポートしています。

ポートベーストランクでは、トランクケーブル間のトラフィックの割り当ては、物理的ポートに基づいて行われます。

トラフィックの割り当てはスイッチによる自動、または管理者が手動で設定することができます。MAC ベースとランクでは、トランクケーブル間のトラフィックの割り当ては、トラフィックの MAC アドレスに基づいて行われます。

2.12.1 ポートベーストランク

Trunk

Disable　Port-Based　Mac-Based

Trunking Group Configuration

Grp#	Candidate Ports	Member selection							
		1	2	3	4	5	6	7	8
3	1, 2, 3, 4, 5, 6, 7, 8	☐	☐	☐	☐	☑	☑	☐	☐

Apply

Forwarding Map

Auto map　Manual map

Port Routing	1	2	3	4	7	8	9	10
Port 5	○	○	○	○	○	○	○	○
Port 6	○	○	○	○	○	○	○	○

設定・表示項目

本機は 4 つのトランクグループをサポートしています。トランクグループは初期状態では無効になっています。

トランク機能を使用したい場合は、下記の手順に沿って設定してください

(1) "Port-based" を選択します。

(2) トランクにポートを割り当て、[Apply] をクリックします。トランクが作成されました。

(3) "Forwading Map" で "Auto map" または "Manual map" を選択します。

(4) "Manual map" を選択した場合、トランクポートにユーザーポートを割り当てます。ユーザーポートから来たトラフィックはトランクポートのトランクケーブルを通過します。

(5) トランクからポートを除きたい場合、ポートのチェックを外し [Apply] をクリックします。

2.12.2　MAC ベーストランク

Trunk

Disable　Port-Based　Mac-Based

Trunking Group Configuration

Grp#	Candidate Ports	Member selection
3	1, 2, 3, 4, 5, 6, 7, 8	1 2 3 4 5 6 7 8 Apply

Giga Port Trunking :　9/G1,10/G2

Distribution Hashing Key :　Destination Address　Source Address　Both

Apply

設定・表示項目

本機は 4 つのトランクグループをサポートしています。トランクグループは初期状態では無効になっています。MAC ベーストランク機能を使用したい場合は、下記の手順に沿って設定してください。

(1) "MAC-Based" を有効にする。

(2) トランクにポートを割り当て、[Apply] をクリックします。トランクが作成されました。

(3) キーを、"Destination Address"、"Souce Address" または "Both" から選択します。

(4) ギガビットポートをトランクに使用する場合、"Giga Port Trunking" で "9/G1,10/G2" にチェックを入れます。

(5) トランクからポートを除きたい場合、ポートのチェックを外し [Apply] をクリックします。

[注意]　トランク機能を無効にしたい場合、"Disable" を選択して [Apply] をクリックしてください。スイッチはトランク設定を削除します。

関連する項目

trunk ートランク（P18）

2.13 IGMP

IGMP

IGMP ○ Enable ⦿ Disable

Port Number	1	2	3	4	5	6	7	8	9	10
Router Port	⦿	○	○	○	○	○	○	○	○	○

Apply

Members Group Total : 0

Total page : 1 Current page : 1 Go to page : Apply Previous Page Next Page

Group	Group Address	Members Port

設定・表示項目

IGMP 機能はネットワーク上での IP マルチキャストの動作のために使用されます。

（1）IGMP を有効にします。

（2）"Router Port" を選択します。

（3）[Apply] をクリックし、設定を適用します。

学習された IP マルチキャストグループは "Member Group" にて確認ができます。

2.14 802.1x 設定

802.1x Configuration

Authentication Configuration		
802.1x System Authentication Status	Disable	
Re-authentication	Disable	
Re-authentication Timeout Period	3600	(0..65535) seconds
Re-authentication Max Count	2	(1-10)
Max Request Count	2	(1-10)
Server Timeout Period	30	(0..65535) seconds
Supplicant Timeout Period	30	(0..65535) seconds
Quiet Timeout Period	60	(0..65535) seconds
Tx Timeout Period	30	(0..65535) seconds

Apply

Radius Server Configuration	
Radius Server IP Address	192.168.1.222
Radius Server Port Number	1812
Security Key	12345678

Apply

802.1x 機能は認証されたユーザーのみにポートへのアクセスを制限することができます。認証プロセスのため RADIUS サーバーが必要です。また本機はオーセンティケーターとして動作します。

設定・表示項目

802.1x System Authentication Status (Enable/Disable/Transparent)

- Enable ー認証モードで 802.1x 機能を有効にします。
- Disable ー 802.1x 機能を無効にします。802.1x プロトコルのパケットは破棄されます。
- Transparent ー 802.1x プロトコルのパケットは転送されますが、認証機能は動作しません。

[注意] 802.1X と MAC セキュリティは同時に動作されることができません。802.1X 機能を有効にする場合、最初に MAC セキュリティ機能を無効に設定してください。

Re-authentication (Enable/Disable)
ユーザーの再認証機能を有効にします。

Re-authentication Timeout
ここで設定された秒数経過するとユーザーの再認証を行います。

Re-authentication Max Count
スイッチとユーザーの間で行う認証の最大試行回数を設定します。

Max Request Count
スイッチと RADIUS **サーバーの間で行う認証の最大試行回数を設定します。**

Server Timeout Period

スイッチと RADIUS **サーバーの間でリクエストがタイムアウトするまでの秒数を指定します。**

Supplicant Timeout Period
これは最初の認証の後、スイッチとユーザー（802.1x **の用語でユーザーはサプリカントと呼びます）間がタイムアウトするまでの秒数です。値の範囲は** 0 〜 65535 **です。**

Quiet Timeout Period
認証が失敗したとき、次の認証プロセスに移る前にスイッチとユーザー間で 802.1x **が動作しない秒数です。**

Tx Timeout Period
これはスイッチからユーザーへの認証リクエストがタイムアウトするまでの秒数です。リクエストは Re-authentication Max Count **で設定した回数になるまで再送信されます。その後、認証失敗のメッセージが送信されます。値の範囲は** 0 〜 65535 **です。**

Radius Server IP Address
RADIUS **サーバーの** IP **アドレスを指定します。**

Radius Server Port Number
RADIUS **サーバーのポート番号を指定します。**

Security Key
RADIUS **サーバーとの認証に使うセキュリティキーを指定します。**

Port Authentication Configuration

Port	Status	Authentication Mode
1	-	Force-Authorized
2	-	Force-Authorized
3	-	Force-Authorized
4	-	Force-Authorized
5	-	Force-Authorized
6	-	Force-Authorized
7	-	Force-Authorized
8	-	Force-Authorized
9	-	Force-Authorized
10	-	Force-Authorized

Apply

"Port Authentication Configuration" **では本機のそれぞれのポートに認証モードの設定を行います。**

設定・表示項目

Auto
通常の 802.1x 動作モードです。それぞれのポートで認証が行われます。

Force-Authorized
このモードは、ポートが常に 802.1x の認証が成功したものであると強制します。実際の認証結果は無視されます。

Force-Unauthorized
このモードは、ポートが常に 802.1x の認証が失敗したものであると強制します。実際の認証結果は無視されます。

None
このモードは設定したポートで 802.1x の動作を無効にします。

[注意] 本ページでは、各設定グループごとに [Apply] ボタンがあり、項目ごとに [Apply] を行う必要があります。例えば、”Authentication Configuration” の設定を行った後、[Apply] ボタンを押さずに ”Radius Server Configuration” を行い ”Radius Server Configuration” の [Apply] をクリックすると、”Authentication Configuration” で行った設定は適用されず、初期状態に戻ってしまいます。各グループの設定を行うごとに [Apply] ボタンで設定を適用してください。

2.15　ポート統計情報

Statistics

Destination Port	7	Refresh Interval (5 - 60) secs	30

Rx Counter	Statistics
Good Unicast Frame	1400
Good Broadcast Frame	131
Good Multicast Frame	43
802.3X MAC Control	0
Total Receive Byte Count	187417
CRC Error	0
Fragment	0
Jabbers	0
Tx Counter	**Statistics**
Good Unicast Frame	1365
Good Broadcast Frame	0
Good Multicast Frame	0
802.3X MAC Control	0
Total Transmit Byte Count	963824

Refresh　Reset Statistics

このページではトラフィックの統計を見ることができます。違うポートのカウンタを取得する場合はポート番号を選択してください。

カウンタの更新間隔を変更するには ”Refresh Interval” の値を変更します。[Refresh] ボタンをクリックするとすぐにカウンタをアップデートすることができます。

[Reset Statistics] ボタンを押すとカウンタをゼロにリセットすることができます。

2.16 システム管理

Maintenance Tools

System Upgrade

Enter the path and name of the upgrade file then click the "START" button .

参照... START

System Backup

Please press the " Backup Setting " button to save the configuration data to your pc .

Backup Setting

Enter the path and name of backup file then press "Restore Setting" button .

参照... Restore Setting

System Restore Factory Default Settings

Please press the " Restore " button to restore the factory default settings of the Device .

Restore

System Reset

In the event that the Device stops responding correctly or in some way stops functioning, you can perform a reset. Please press the " Reset " button

Reset

本機はシステム管理ツールとして 4 つの機能をサポートしています。

System Upgrade

Web マネージメント PC 経由で、システムオペレーションソフトウェアのアップグレードを行います。

System Backup

– Backup Setting
設定ファイルを、Web マネージメント PC 経由でバックアップします。

– Restore Setting
Web マネージメント PC から、設定のバックアップファイルを取得し、本機の設定をリストアします。

System Restore Factory Default Setting

本機の設定を工場出荷状態に戻します。

System Reset

本機をリセットします。

FXC3009 Management Guide (FXC08-DC-200027-R1.0)

初版　　2008 **年** 12 **月**

FXC3009 Management Guide

FXC株式会社